

REMARKS

I. Interview Summary

Applicant acknowledges, with appreciation, the telephonic interview conducted on June 2, 2010 between the undersigned and Examiner Chen, to discuss the rejections of the pending claims. The substance of the interview is reflected in the remarks below.

II. Amendments to the Claims

Applicant acknowledges, with appreciation, withdrawal of previous objection to the drawings and previous rejection of claims 24-41 and 43-46 under 35 U.S.C. § 112, first paragraph. Claims 24-41 and 43-46 are pending and under examination. Applicant amends claims 24, 27, 29, 39, and 46, as detailed in the listing of claims. The amendments to claims 24 and 39 are supported by Applicant's specification at, for example, page 3, lines 6-34, and page 5, lines 22-30. Further, the amendments to claims 27 and 29 include rewriting these claims as independent claims and incorporating some elements of claim 24. No new matter has been introduced by these amendments.

III. Office Action

Applicant respectfully traverses the rejections set forth in the Office Action, wherein the Examiner rejected claims 24-41 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,177,425 ("Ben") in view of U.S. Patent Application Publication No. 2004/0204124 ("Campbell").

IV. Response to Rejections

Applicant requests reconsideration and withdrawal of the rejection of the pending claims under 35 U.S.C. § 103(a) as being unpatentable over Ben in view of Campbell. The Final Office Action has not properly resolved the *Graham* factual inquiries, the proper resolution of which is

the requirement for establishing a framework for an objective obviousness analysis. *See* M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), as reiterated by the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). Specifically, as described below, the Final Office Action has not properly ascertained the differences between the claimed invention and the prior art, at least because the Final Office Action has not interpreted the prior art and considered both the invention and the prior art as a whole. *See* M.P.E.P. § 2141(II)(B).

Independent Claims 24 and 39

The cited references, whether considered alone or in combination, at least do not teach or suggest a “method for cipher-controlled exploitation of data resources stored in a remote database associated with a computer system,” which comprises:

providing a subscriber identity module carrying at least one security algorithm, said subscriber identity module not used, either directly or indirectly, by said computer system for communication with a network;

producing a cipher key via said at least one security algorithm;

using said cipher key for protecting said data resources; and

storing said protected data resources in said remote database in an encrypted format,

as recited in claim 24 (emphases added).

As recited in claim 24, a subscriber identification module (SIM) is used for “the cipher controlled exploitation of data resources ... associated with a computer system,” which does not use the SIM, either directly or indirectly, for communication with a network. Applicant’s specification discusses the problem of protecting sensitive and valuable information in a computer system. See, e.g., Applicant’s specification at, for example, page 1, lines 15-30. Further, Applicant’s specification describes other references in which the SIM of a mobile

phone is utilized for logging a user into a computer system, or for generating a copy of a key used in accessing resources. See id. at, for example, page 1, line 31 to page 2, line 32.

On the other hand, Applicant's specification¹, in some embodiments, "provid[es] an arrangement implementing a secure and low-cost method for protecting any sensitive data stored in a computer system and/or a local access to the computer system itself ... by means of a SIM (Subscriber Identity Module)." Id. at page 3, lines 6-12 (emphases added). Some embodiments, for example, take advantage of the existing security functions of a SIM (see, e.g., Id. at lines 21-23) used in a mobile device that can communicate with a mobile network (see, e.g., Id. at page 3, lines 13-20; page 5, lines 31-34), to solve a client security problem of a computer system that is not necessarily associated with that mobile network, and is not using the SIM for its communication with a network (see, e.g., Id. at page 5, lines 22-30). Instead, the computer system may be interfaced with the SIM through one or more of various technologies, unrelated to the communication of the computer system with a network. See, e.g., Id. at page 7, lines 18-28.

On pages 2-3, the Office Action asserted that Ben discloses all the elements of pending claim 24 except for "a remote storing location accessible by said user via a communication network," and relied on Campbell to cure the admitted deficiency of Ben. However, Ben is missing other features as well, and Campbell does not supply those missing features. Specifically, Ben uses a SIM to secure the information on the communication device that uses that SIM for communication with a network. See, e.g., Ben at Abstract.

The Office Action asserted that in Ben "the SIM card is used to generate cipher keys for encryption, not directly used for communication with a network." Office Action at 3 (emphasis added); see also Office Action at 8. Applicant respectfully disagrees. In Ben, the SIM card is

¹ References to Applicant's specification are exemplary in nature and in no way intended to limit the scope of the claims.

used by the communication device for two purposes, i.e., to generate cipher keys and to communicate with a network. Ben describes that “[t]aking the present mobile phone as an example, the user generally needs to insert the Subscriber Identity Module (SIM) card to start the communicating function of the mobile phone. The SIM card usually has the function of generating a cipher key.” Ben at column 1, lines 24-28 (emphasis added). Moreover, Ben describes that “[t]he first method according to the prior art takes advantage of the SIM card to secure private information associated with the subscriber. However, the first method according to the prior art only secures private information that stored in the SIM card, without securing the information stored in the mobile phone.” Id. at lines 37-42. In Ben, on the other hand, “a primary objective ... [is] to provide a device for securing private information associated with the subscriber in a communication apparatus.” Id. at lines 63-65. To that end, Ben takes advantage the SIM, used in the communicating function of the device, to also generate a cipher-key used in its encryption system:

It is am [sic] advantage of the present invention that the communication apparatus comprises a cipher-key generating module, such as subscriber information module card, SIM card. The device retrieves the cipher key through the cipher-key generating module to encrypt or decrypt the information associated with the subscriber; therefore, secures the information associated with a subscriber.

Id. at column 2, lines 29-35 (emphasis added).

Therefore, contrary to the assertions by the Office Action, the SIM in Ben is used by Ben’s device for communication with the network. However, to further distinguish Ben, and pursuant to a suggestion by the Examiner during the telephone interview of June 2, 2010, Applicant has amended claims 24 and 39 to recite that the claimed SIM is not used, either directly or indirectly, by the claimed computer system for communication with a network. As explained above, Ben does not teach or suggest these elements.

Campbell does not cure the deficiencies of Ben. Campbell is directed to improving wireless devices via limiting the quantity of information stored on the wireless devices by uploading some of that information to a remote server database. See, e.g., Campbell at Abstract. Therefore, similar to Ben, Campbell is also directed to utilities implemented in a communication device and is concerned with information stored in that communication device. Nowhere does Campbell teach or suggest using a subscriber identity module for any purpose.

Independent claim 39, although differing in scope from claim 24, recites features similar to those discussed above in relation to claim 24. Specifically, claim 39 recites a

system for cipher-controlled exploitation of data resources, comprising at least one subscriber identity module [SIM] carrying at least one security algorithm; [and] at least one computer system comprising at least one processing module, said subscriber identity module not used, either directly or indirectly, by said at least one computer system for communication with a network and said at least one processing module being interfaced with said at least one subscriber identity module to generate a cipher key via said at least one security algorithm and being configured to protect via said cipher key said data resources.

(Emphasis added).

Therefore, independent claims 24 and 39 are not obvious and should be allowable.

Independent Claim 27

During the interview of June 2, 2010, Examiner Chen indicated that claim 27 may contain allowable subject matter. In response thereto, Applicant has rewritten claim 27 as an independent claim and has incorporated in claim 27 some elements of claim 24. Applicant contends that claim 27 is also patentable over the cited references, because Ben and Campbell, whether considered separately or in combination, do not teach or suggest a “method for cipher controlled exploitation of data resources stored in a remote database associated with a computer system,” which comprises, among other things:

generating at least two random values;

subjecting said at least two random values to ... at least one security algorithm to generate at least two session keys; [and]

combining said at least two session keys via a mixer function to produce a cipher key;

using said cipher key for protecting said data resources;

as recited in claim 27 (emphases added).

In its rejection of claim 27, on pages 4-5, the Office Action cited column 5, lines 4-15 of Ben. Applicant, however, respectfully notes that the cited section in Ben, or any other section, does not teach or suggest the above features of claim 27. Specifically, the cited section merely describes various modules of a secure device including a random generating module, which, in each operation, generates one random input, used by a cipher-key generating module to generate a cipher key. Ben or Campbell do not teach or suggest “generating at least two random values ... generat[ing] at least two session keys, ... and combining said at least two session keys via a mixer function to produce [one] cipher key,” as recited in claim 27 (emphases added). Therefore, for at least the above reasons, claim 27 is also nonobvious and should be allowable over the cited references.

Independent Claim 29

During the interview of June 2, 2010, Examiner Chen also indicated that claim 29 may contain allowable subject matter. In response thereto, Applicant has also rewritten claim 29 as an independent claim and has incorporated in claim 29 some elements of claim 24. Applicant contends that claim 29 is also patentable over the cited references, because Ben and Campbell, whether considered separately or in combination, do not teach or suggest a “method for cipher controlled exploitation of data resources stored in a remote database associated with a computer system,” which comprises, among other things:

generating at least one random value;

subjecting the at least one random value to ... [a] security algorithm to generate at least one session key;

providing a mixer function;

inserting in the mixer function a user specific secret unrelated to said subscriber identity module security algorithm;

processing the at least one session key via the mixer function to produce a cipher key,

as recited in claim 29 (emphases added).

As examples of the above features, Applicant's specification, in some embodiments, provides an added security measure in which "the mixer function f can include a user specific secret key K_u [in addition to session keys K_c derived as functions of random values] in order to make the encryption key K unpredictable also for the mobile operator, which usually knows the key K_i embedded into the SIM." Applicant's specification, p. 14, lines 32-35 (emphasis added). See also, Applicant's specification at page 10, lines 22-30; page 14, line 32 to page 15, line 2.

In the rejection of claim 29 on page 5, the Office Action cited column 3, lines 28-37 of Ben. However, the cited section merely describes that the cipher-key generating module in Ben can be a SIM, and that, instead of using a predetermined algorithm in SIM to generate a cipher key, Ben's system can use a previously stored subscriber code, such as International Mobile Subscriber Identity (IMSI) as a cipher key. See Ben column 3, lines 28-37. However, an IMSI can not correspond to the recited user specific secret, e.g., K_u , because, unlike K_u , IMSI is embedded into the SIM. Moreover, Ben does not teach or suggest that the IMSI, or any user specific secret, is inserted in a mixer function to produce an encryption key, as required by claim 29. Instead, Ben directly uses the IMSI as its cipher key.

Campbell does not cure the above deficiencies of Ben, because Campbell, also, does not teach or suggest "inserting in [a] mixer function a user specific secret unrelated to [a] subscriber

identity module security algorithm; [and] processing ... at least one session key via the mixer function to produce a cipher key,” as recited by claim 29.

Therefore, for at least the above reasons, claim 29 is also nonobvious and should be allowable over the cited references.

Claim 34

Claim 34 depends, indirectly, from claim 24, and therefore includes features of claim 24 discussed above. Also, claim 34 recites a method in which “said cryptographic header [of the data in encrypted format] comprises an identifier of said subscriber identity module [SIM] and a cryptographic checksum based on said cipher key, said cryptographic checksum being used for detecting any unauthorized modifications of said encrypted format” (emphasis added). As an exemplary illustration of this feature, Applicant’s specification illustrates the cryptographic header and its fields in Fig. 3 and its detailed description.

In its rejection of claim 34 on page 6, the Office Action cited column 5, lines 21-25 of Ben. However, the cited section merely describes that the cipher-key generating module in Ben can be a SIM, and that the predetermined calculating algorithm in Ben can be a HMAC, GSM-A3, or GSM-A8. This section or any other section of Ben does not teach or suggest an encrypted data which includes a cryptographic header comprising a cryptographic checksum, as recited in claim 34. Therefore, for at least the above reasons, claims 34 is also nonobvious and should be allowable over the cited references.

Remaining Claims

Dependent claims 25, 26, 28, 30-33, 35-38, 40, 41, and 43-46 should also be allowable at least by virtue of their respective dependence from base claim 24 or 39, and also because they recite additional features not taught or suggested by the cited references.

V. Conclusion

Applicant respectfully requests the reconsideration and withdrawal of the rejections, and the timely allowance of the pending claims.

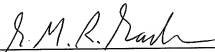
The Office Action contained a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Final Office Action.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 28, 2010

By: 
Reza Sadr, Ph.D.
Reg. No. 63,292
(617) 452-1653